STATEMENT OF
LESTER J. JOHNSON JR.

SCANA CORPORATION
CORPORATE SECURITY MANAGER FOR INVESTIGATIONS AND CRISIS MANAGEMENT

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY ON INTELLIGENCE
INFORMATION SHARING AND TERRORISM RISK ASSESSMENT
"PRIVATE SECTOR INFORMATION SHARING: THE DHS PERSPECTIVE AND LESSONS LEARNED"

THURSDAY, JULY 26, 2007
ROOM 311 CANNON HOUSE OFFICE BUILDING

Madam Chairwoman Harman, Ranking Member Reichert, and distinguished members of the subcommittee, I appreciate the invitation to appear before you today, as it is both an honor and a privilege to be here today. I would respectfully request that my written testimony be submitted into the record. I appear before you today to share some insights I believe are critical to the private sector information sharing and to highlight those areas in need of improvement and those which are on the path to success. The private sector currently has sole possession of approximately eighty-five percent of the vital critical infrastructure in existence today, upon which all of us depend on daily. For a number of years now, we have been focusing on how to build trusted relationships and processes to facilitate information sharing; overcome barriers to information sharing, clarifying roles and responsibilities of the various government and private sector entities that are involved in and charged with protecting critical infrastructures. In order to protect our nation's critical infrastructure and key assets (CI / KA), the full support, cooperation and engagement of Government and the private sector partners at all levels is required.

I have the unique opportunity to speak to this issue from both the government and private sector due to my previous employment history with the South Carolina Law Enforcement Division (SLED) and my current employer in the private sector. I had the opportunity to participate in the delivery of services with respect to Homeland Security in South Carolina as SLED is the designated agency responsible for Homeland Security and Chief Robert M. Stewart serves as the State Homeland Security Advisor.

The importance of trusted relationships between Government and private sector in South Carolina has been recognized and established on several levels. Private sector representation exists on both the regional and state Counter Terrorism Councils and in the all source Fusion Center. I will elaborate more on these initiatives later in my testimony. Below, I will be identifying areas of both concern and success, as it is my intent to be a part of the solution to these areas.

Information Flow:

The flow of information between the Government and private sector are interpreted to be a one way investment for the private sector. While there is a great effort on the Government's part to solicit situational awareness, timely and actionable and proprietary information from the privates sector, there still exists a significant deficiency on the Government's part to share the information back to the private sector. Information provided by the private sector with regard to suspicious activity is received by the Government and subjected to an analytical process which I am told includes a human and technological assessment, often taking weeks or months to complete. During this time, the information is not shared among the peers of the sector due to the lack of a complete analysis being available. Disparately, should the same information be collected by a peer member who does not forward it to the Government, there is no link identified since the Government chooses to hold the information instead of sharing it across the sector. The process I described creates an atmosphere of difficulty for the private sector to adequately place a remediation plan into effect.

I made a valiant effort to seek input from my peers in the industry who are not present here today before the committee. I have been educated on several instances where information was discovered; often months after the Government learned it, where no one the industry was made aware of an existing threat or vulnerability that could have an enormous negative impact on the industry.

Portal Fatigue:

The industry as a whole has been besieged by the number of information sharing portals from the various Government agencies and some private as well, in attempt to go and find the information. Each portal has a separate vetting process which must be adhered to, a separate user name and password, a unique URL, and to some degree each contains the same information with regard to its informational value to the user. As I am sure you aware, in the private sector, time is equated to money. There is no

effort among the Government to coordinate the efforts among the various agencies to simplify this process in any way. Actually, there appears to be competition to see which agency can turn out the most portals in a given amount of time. The idea of posting the information, particularly information with no or little classification, to site for all to come to is at best a backwards approach to information sharing. One would consider the Government as the provider of information in this scenario, yet the provider creates technology requiring the end user to come to the Government instead of the Government pushing the information to the end user. A definite confusing demonstration of a product chain and certainly one the private sector is weary of. Perhaps consideration may be given to using the existing technology to develop a "role based security dashboard" atmosphere. A role based security dashboard would have an individual vetted for all the existing Government portals. The Government would then feed the information into a dashboard which would be accessed by the end user. All the information pushed to the dashboard would be available at one location, requiring one user name and password, and would provide a timely and accurate assessment of all information and could also provide tools for data mining the information based on the user instead of the provider.

Private Sector Information Sharing:

The private sector has found success in utilizing services from other private sector organizations that provide situational awareness and information on a variety of topics and services. These services, while costly to an organization, are very timely and efficient. The services allow the sector to choose the type of information they wish to receive and allow information to be vetted by the distance from a facility or city. I have personal experience with one such organization and found the services to be very beneficial. These organizations leverage technology in various formats to push this desired information out to the end user and have demonstrated an uncanny ability to learn of potential threats, delays and risks in record time.

I am forced to rely on the open sources of information to receive most of the situational awareness information available. I have found a television tuned to a cable news network provides the most efficient, timely and accurate information to my company. Considering the amount of investment our country has made toward the sharing of information among our Government agencies and the public sector, I find this reprehensible. We certainly are capable of embracing technology and conducting ourselves better than this. At a minimum, perhaps the Government should consider contracting the services of one of companies who have perfected this and make the services available to the end users who require it. The

Southeastern Emergency Response Network is another example of a creation of a private sector initiative which became necessary due to the failure of a Government effort. Homeland Security Information Network – XXX was an original effort to provide a means of information sharing between the Government and private sector. I was approached on the State's behalf to develop the program in South Carolina. I received the organizational chart for the critical infrastructure and contacted our local private sector and sought the commitment to serve in the leadership capacity for the required vetting among the sectors. Once in place, I delivered the chart as requested only to find there had been technological setbacks that would delay the initiation of the project. Some years later I was finally notified that the program would be replaced with anew program which to date has yet to be introduced.

Many of my peers and I have begun a very basic method of information sharing among ourselves as a result of not receiving the intelligence we desire from our Government sources. We have resorted to a telephone tree of sorts to ensure each of us share the information in a timely fashion and develop actionable plans for remediation where appropriate.

Dam Sector Working Group:

Several members of our industry were recruited to participate in a working group to develop the Homeland Security Information Network – Dam Sector (HSIN-DS) and the Asset Identification Database. These efforts were met with great enthusiasm by the sector and several individuals provided a great amount of resources toward this effort. Unfortunately, the Government has not provided the same level of enthusiasm and effort. As a result the project has been at a stand still for some period of time. Initially, there were technology setbacks which over time were able to be corrected. The vetting process presented difficulties over which process would be used by both entities. Due to difficulties arising from the PCII, private sector representatives are skeptical about placing the information into the system. As you can see, there are a number of issues outstanding concerning this project, which is paramount to the safety of one of our most critical infrastructures.

HITRAC:

The creation of a partnership between the Department of Homeland Security's Office of Infrastructure Protection and the Officer of Intelligence and Analysis to provide a tailored risk assessment product for CI / KR sectors fusing consequence and vulnerability information with threat information is an excellent plan of action. We continue to fall short on the

timely sharing of the information generated from this program. We have been told to expect informational bulletins, analytical reports and annual reports and to date we have not received any. The sectors can only respond to strengthen and protect our infrastructure if we receive the information derived from the process below. Without the benefit of this, we have relied heavily on our own resources and our peers for information. Additionally, the lack of communication creates a large void of information flow from the private sector to the Government.

Infrastructure Information and Collection Program:

The Protected Critical Infrastructure Information (PCII) has failed to demonstrate the Government has the ability to provide a safe and secure atmosphere for descriptive and proprietary information to exist in a repository. Efforts to identify and prioritize national and sector level CI / KR information have yet to demonstrate to the private sector that the information can be maintained in a confidential manner. Recently, this was demonstrated to a peer of mine while attending a meeting, at which time a document that had been provided under the protection of this program was produced by an individual who should not have had access to the document. Incidents such as this are many and cause the private sector to withhold information which in any way may be considered private or proprietary.

South Carolina All Source Fusion Center:

Among the difficulties we face every day, there are efforts which demonstrate the success and progress we have reached at the State and local level. The creation of the Fusion center in South Carolina is a foundation for the development of a trusted relationship between Government and the private sector. I received notification only three days ago that the Department of Homeland Security State and Local intelligence Community of Interest has cleared the way for private sector representatives to be co-located within the State Fusion Center. A program such as this will greatly enhance the flow of information between Government and the private sector.

South Carolina Information Exchange:

Homeland Security in South Carolina developed the South Carolina Information Exchange (SCIEx) within the State operated all source Fusion Center. SCIEx is an excellent example of information sharing in a near real time environment. Law Enforcement agencies within the state have

participated in this project by allowing the information contained in incident reports created in an automated environment to be replicated to a data warehouse with SLED and allowing for the querying of the information contained therein through a secure web browser. The sharing of this information is a tremendous resource for both the state and the private sector. Information derived from these reports can easily be placed into geographical information software and immediately demonstrate a potential threat and vulnerability to our facilities throughout the state. The technology for accomplishing this feat was developed with the assistance of the National Law Enforcement and Corrections Technology Center – Southeast, which is funded in part by the National Institute of Justice. The software code for this is an open source product, making it available to entities free of charge, resulting in the State of Tennessee initiating a project to replicate the success there as well. I have no reservation recommending this technology be used to better facilitate information sharing among the private sector. There is a success there waiting to happen without the demand of additional tax dollars and development time.

Conclusion:

In conclusion, I feel that it is imperative for the committee to understand the commitment and dedication of the private sector has with regard to the sharing of information. We realize there are great benefits to be reaped by both the sector and the Government in the presence of a trusted partnership. There have been many, too many actually, attempts to develop and implement a program where this type of exchange can be conducted and the information shared can be relayed and maintain the integrity necessary for the public sector. I and many of my peers are fully prepared to again tackle these difficult issues so long as there is the same level of commitment from our Government counterparts. Until such time, we will continue to make progress with our State Government partners and our industry peers to ensure we have the necessary information to complete our duty to protect the critical infrastructure of the United States of America.

Follow Up Address:

Lester J. Johnson Jr.
1426 Main Street Mail Code: 020
Columbia, South Carolina 29201
(803) 217-9079